ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАЩИТА ИНФОРМАЦИИ

# ИСПЫТАНИЯ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ

## ТИПОВОЕ РУКОВОДСТВО

Издание официальное

БЗ 9—97/306

ГОССТАНДАРТ РОССИИ
Москва

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН 27 Центральным научно-исследовательским институтом Министерства обороны Российской Федерации (27 ЦНИИ МО РФ) и Научно-консультационным центром по созданию и применению информационных технологий (НКЦ «ЦНИИКА-СПИН»)

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 14 июля 1998 г. № 295

3 ВВЕДЕН ВПЕРВЫЕ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Защита информации**

# ИСПЫТАНИЯ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ

**Типовое руководство**

Information security. Software testing for the existence of computer viruses. The sample manual

**Дата введения 1999—07—01**

## 1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящий стандарт распространяется на испытания программных средств (ПС) и их компонентов, цели которых — обнаружить в этих ПС и устранить из них компьютерные вирусы (КВ) силами специальных предприятий (подразделений), и устанавливает общие требования к организации и проведению таких испытаний.

1.2 Требования, установленные настоящим стандартом, направлены на обеспечение специальной обработки ПС в целях выявления КВ, а также на устранение последствий, вызванных возможными воздействиями КВ на операционные системы, системные и пользовательские файлы с программами и данными, начальные секторы магнитных дисков, таблицы размещения файлов и др.

1.3 Настоящий стандарт устанавливает типовые требования, предъявляемые к испытаниям ПС на наличие КВ, в том числе:

- к составу мероприятий по подготовке и проведению испытаний;
- к составу, структуре и назначению основных частей программно-аппаратного стенда, обеспечивающего проведение испытаний;
- к выбору и использованию методов проведения испытаний;
- к тестовым (антивирусным) программам, обнаруживающим и уничтожающим КВ;
- к составу и содержанию документации, фиксирующей порядок проведения испытаний и их результаты.

1.4 Настоящий стандарт предназначен для применения в испытательных лабораториях, проводящих сертификационные испытания ПС на выполнение требований защиты информации.

## 2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящем стандарте использована ссылка на следующий стандарт:

ГОСТ 19.301—79 (СТ СЭВ 3747—82) ЕСПД. Программа и методика испытаний. Требования к содержанию и оформлению

## 3 ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем стандарте применены следующие термины с соответствующими определениями:

**Защита программных средств** — организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий.

**Сертификация** — действия третьей стороны, цель которых — подтвердить (с помощью сертификата соответствия) то, что изделие (в том числе программное средство) или услуга соответствует определенным стандартам или другим нормативным документам.

**Профилактика** — систематические действия эксплуатационного персонала, цель которых — выявить и устранить неблагоприятные изменения в свойствах и характеристиках используемых программных средств, в частности проверить эксплуатируемые, хранимые и (или) вновь полученные программные средства на наличие компьютерных вирусов.

**Издание официальное**

★

**Ревизия** — проверка вновь полученных программ специальными средствами, проводимая путем их запуска в контролируемой среде.

**Несанкционированный доступ к программным средствам** — доступ к программам, записанным в памяти ЭВМ или на машинном носителе, а также отраженным в документации на эти программы, осуществленный с нарушением установленных правил.

**Вакцинирование** — обработка файлов, дисков, каталогов, проводимая с применением специальных программ, создающих условия, подобные тем, которые создаются определенным компьютерным вирусом, и затрудняющих повторное его появление.

**Компьютерный вирус** — программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

В настоящем стандарте приняты следующие сокращения:

- ПС — программные средства.
- КВ — компьютерные вирусы.
- ПЭВМ — персональная электронно-вычислительная машина (персональный компьютер).
- ЭВМ — электронно-вычислительная машина.

## 4 ПОРЯДОК ПРОВЕДЕНИЯ ИСПЫТАНИЙ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ

4.1 Испытания ПС на наличие КВ следует проводить на специально оборудованном программно-аппаратном испытательном стенде, в составе которого должны быть необходимые технические и программные средства, в том числе антивирусные программы.

4.2 Предприятие [подразделение (далее — организация)], проводящее проверку ПС на наличие КВ, должно поддерживать испытательный стенд в работоспособном состоянии и не допускать проникновения КВ в программы и данные до начала проведения испытаний.

4.3 Организация, проводящая проверку ПС на наличие КВ, должна определить и зафиксировать в программе испытаний цель и объем испытаний, а также свои обязательства, касающиеся мер защиты проверяемых ПС от их заражения КВ с учетом требований ГОСТ 19.301.

4.4 Меры по защите проверяемых ПС от заражения КВ могут включать в себя:

- разработку и выполнение комплекса мероприятий по профилактике, ревизии и вакцинированию используемых ПС;
- подготовку должностных лиц, отвечающих за проведение испытаний ПС;
- разработку и выбор способов применения программно-технических средств для обнаружения КВ в ПС;
- взаимодействие организаций, заказывающих и проводящих испытания ПС;
- контроль за проведением испытаний ПС;
- оценку эффективности применяемых антивирусных средств;
- совершенствование системы мероприятий по защите ПС от КВ на основе современных достижений информационной технологии;
- установление административной ответственности должностных лиц за выполнение требований защиты ПС от КВ;
- назначение ответственных должностных лиц и определение их полномочий, относящихся к организации и проведению мероприятий по защите ПС от КВ.

4.5 Организация, выполняющая проверку ПС на наличие КВ, должна обеспечить весь процесс проверки необходимыми вычислительными техническими и программными средствами, а также назначить специально обученных сотрудников для проведения испытаний.

4.6 Организация, выполняющая проверку ПС на наличие КВ, должна назначить постоянного представителя, который получает определенные полномочия и несет постоянную ответственность за выполнение требований, установленных настоящим стандартом.

4.7 В состав технических средств испытательного стенда должны входить:

- совместимые ПЭВМ;
- необходимые элементы телекоммуникационных сетей;
- каналы связи.

4.8 Конкретный набор технических компонентов испытательного стенда должен быть таким, чтобы были обеспечены условия воспроизведения всех необходимых внешних воздействий на ПС в процессе проведения испытаний.

Перед началом испытаний состав технических средств, используемых для проведения проверок ПС на наличие КВ, должен быть согласован с организацией, заказывающей эти проверки. При этом согласование должно быть оформлено соответствующим актом.

4.9 Наряду с компонентами, указанными в 4.7, в состав испытательного стенда могут входить соответствующие аппаратные антивирусные средства. К ним относятся:

- компьютеры специальной конструкции, благодаря которой несанкционированный доступ к данным и заражение файлов КВ могут быть существенно затруднены;
- специальные платы, подключаемые к одному из разъемов ПЭВМ и выполняющие те или иные функции защиты информации;
- электронные ключи защиты информации, главным достоинством которых является их многофункциональность.

4.10 Состав и функциональное назначение программных средств испытательного стенда определяются системой защиты, применяемой при проведении испытаний ПС на наличие КВ.

4.11 Программные средства, входящие в состав испытательного стенда, должны обеспечивать:

- регулярное ведение архивов измененных файлов;
- контрольную проверку соответствия длины и значения контрольных сумм, указываемых в сертификате и полученных программах;
- систематическое обнуление первых трех байтов сектора начальной загрузки на полученных несистемных дискетах;
- другие виды контроля целостности программ перед считыванием с дискеты;
- проверку программ на наличие известных видов КВ;
- обнаружение попыток несанкционированного доступа к испытательным (инструментальным) и (или) испытуемым программам и данным;
- вакцинирование файлов, дисков, каталогов с использованием резидентных программ-вакцин, создающих при функционировании условия для обнаружения КВ данного вида;
- автоконтроль целостности программ перед их запуском;
- удаление обнаруженного КВ из зараженных программ или данных и восстановление их первоначального состояния.

4.12 Состав программных средств, используемых при проведении испытаний по просьбе заказчика, должен быть документально оформлен в соответствии с требованиями заказчика.

4.13 Сроки проведения испытаний должны быть установлены в программе и методике испытаний по договоренности между заказчиком и организацией, проводящей испытания.

4.14 Проверяемые ПС должны быть переданы для испытаний на магнитных носителях (дискетах) вместе с документацией.

4.15 Состав работ по подготовке и проведению испытаний ПС на наличие КВ в общем случае следующий:

- ознакомление с документацией на ПС;
- выбор методов проверки ПС на наличие КВ;
- определение конфигурации программных и аппаратных средств испытательного стенда;
- подготовка программно-аппаратного испытательного стенда к проведению испытаний;
- организация и проведение испытаний;
- оформление протокола проверки ПС и его передача в орган по сертификации в соответствии с 6.2 настоящего стандарта;
- передача заказчику проверенных ПС на магнитных носителях (дискетах);
- установление по согласованию с заказчиком правил (порядка) гарантийного сопровождения проверенных ПС.

4.16 Проверка ПС на наличие КВ в общем случае включает в себя:

- поиск вирусоподобных фрагментов кодов ПС;
- моделирование ситуаций, предположительно способных вызвать активизацию КВ;
- анализ особенностей взаимодействия компонентов ПС с окружающей операционной средой;
- отражение результатов проверки в соответствующей документации.

## 5 МЕТОДЫ ПРОВЕДЕНИЯ ИСПЫТАНИЙ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ

5.1 При испытаниях ПС на наличие КВ используют две основные группы методов обнаружения КВ и защиты программ от них: программные и аппаратно-программные.

К программным методам относятся:

- сканирование;
- обнаружение изменений;
- эвристический анализ;
- резидентные «сторожа»;
- вакцинирование ПС.

Аппаратно-программные методы основаны на реализации любого (любых) из указанных выше программных методов защиты ПС от КВ с помощью специальных технических устройств.

5.2 При выборе методов испытаний и защиты ПС от КВ следует руководствоваться сведениями о сущности каждого из них, приведенными в 5.4—5.9, а также дополнительными пояснениями об их возможностях, достоинствах и недостатках, приведенными в приложении А.

5.3 В конкретных испытаниях могут быть использованы способы и средства обнаружения КВ, реализующие один из методов, указанных в 5.1, или их комбинации.

5.4 Метод сканирования заключается в том, что специальная антивирусная программа, называемая сканером, последовательно просматривает проверяемые файлы в поиске так называемых «сигнатур» известных КВ. При этом под сигнатурой понимают уникальную последовательность байтов, принадлежащую конкретному известному КВ и не встречающуюся в других программах.

5.5 Метод обнаружения изменений заключается в том, что антивирусная программа предварительно запоминает характеристики всех областей диска, которые могут подвергаться нападению КВ, а затем периодически проверяет их. Если изменение этих характеристик будет обнаружено, то такая программа сообщит пользователю, что, возможно, в компьютер попал КВ.

Антивирусные программы, основанные на обнаружении изменений программной среды, называются ревизорами.

5.6 Метод эвристического анализа реализуется с помощью антивирусных программ, которые проверяют остальные программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для КВ. Так, например, эвристический анализатор может обнаружить, что в проверяемой программе присутствует код, устанавливающий резидентный модуль в памяти.

5.7 В методе резидентных сторожей используются антивирусные программы, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. Резидентный сторож сообщит пользователю о том, что какая-либо программа пытается изменить загрузочный сектор жесткого диска или дискеты, а также выполнимый файл.

5.8 Вакцинирование устанавливает способ защиты любой конкретной программы от КВ, при котором к этой программе присоединяется специальный модуль контроля, следящий за ее целостностью.

При этом проверяются контрольная сумма программы или какие-либо другие ее характеристики. Если КВ заражает вакцинированный файл, модуль контроля обнаруживает изменение контрольной суммы файла и сообщает об этом пользователю.

5.9 Аппаратно-программные методы защиты ПС от КВ реализуются с помощью специализированного устройства — контроллера, вставляемого в один из разъемов расширения компьютера, и специального программного обеспечения, управляющего работой этого контроллера и реализующего один или несколько из программных методов, указанных выше.

## 6 ТРЕБОВАНИЯ К ДОКУМЕНТАЦИИ НА ИСПЫТАНИЯ ПРОГРАММНЫХ СРЕДСТВ

6.1 Документация, оформляемая при подготовке и проведении испытаний ПС на наличие КВ, должна содержать сведения, отражающие цель, объем, порядок проведения и результаты таких испытаний.

6.2 Выпуск документа вида «Протокол проверки программных средств на отсутствие компьютерных вирусов» является обязательным. Форму документа «Протокол проверки программных средств на отсутствие компьютерных вирусов» определяют в установленном порядке и передают в орган по сертификации.

6.3 Другие виды документов, выпускаемых по результатам испытаний ПС на наличие КВ, и дополнительные требования к их содержанию определяют по согласованию между организацией, выполняющей проверку ПС, и организацией, заказывающей эту проверку.

6.4 Документация, относящаяся к испытаниям ПС на наличие КВ, может быть представлена на магнитных носителях данных.

*ПРИЛОЖЕНИЕ А*
*(справочное)*

## ПОЯСНЕНИЯ
### о возможностях различных методов обнаружения и устранения компьютерных вирусов

А.1 Сканирование является самым простым программным методом поиска КВ.

Антивирусные программы-сканеры могут гарантированно обнаружить только уже известные КВ, которые были предварительно изучены и для которых была определена сигнатура.

Программам-сканерам не обязательно хранить в себе сигнатуры всех известных КВ. Они могут, например, хранить только контрольные суммы сигнатур. Антивирусные программы-сканеры, которые могут удалить обнаруженные КВ, обычно называются полифагами.

Для эффективного использования антивирусных программ, реализующих метод сканирования, необходимо постоянно обновлять их, получая самые последние версии.

А.2 Метод обнаружения изменений основан на использовании антивирусных программ-ревизоров, которые запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, параметры всех контролируемых файлов, а также информацию о структуре каталогов и номера плохих кластеров диска. Могут быть проверены и другие характеристики компьютера: объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры.

Программы-ревизоры потенциально могут обнаружить любые КВ, даже те, которые ранее не были известны. Однако следует учитывать, что не все изменения вызваны вторжением КВ. Так, загрузочная запись может измениться при обновлении версии операционной системы, а некоторые программы записывают изменяемые данные внутри своего выполнимого файла. Командные файлы изменяются еще чаще; так, например, файл AUTOEXEC. BAT обычно изменяется во время установки нового программного обеспечения.

Программы-ревизоры не помогут и в том случае, когда пользователь записывает в компьютер новый файл, зараженный КВ. При этом, если КВ заразит другие программы, уже учтенные ревизором, он будет обнаружен.

Дополнительной возможностью программ-ревизоров является способность восстановить измененные (зараженные) файлы и загрузочные секторы на основании запомненной ранее информации.

Антивирусные программы-ревизоры нельзя использовать для обнаружения КВ в файлах документов, так как эти файлы постоянно изменяются. Поэтому для контроля за данными файлами следует использовать программы-сканеры или эвристический анализ.

А.3 Эвристический анализ позволяет обнаруживать ранее неизвестные КВ, причем для этого не надо предварительно собирать данные о файловой системе, как требует метод обнаружения изменений.

К основным недостаткам эвристического метода относятся следующие:

- принципиально не могут быть обнаружены все КВ;
- возможно появление некоторого количества ложных сигналов об обнаружении КВ в программах, использующих вирусоподобные технологии (например, антивирусы).

А.4 Большинство резидентных сторожей позволяет автоматически проверять все запускаемые программы на заражение известными КВ. Такая проверка будет занимать некоторое время, и процесс загрузки программы замедлится, но зато пользователь будет уверен, что известные КВ не смогут активизироваться на его компьютере.

Резидентные сторожа имеют очень много недостатков, которые делают этот класс программ малопригодным для использования. Многие программы, даже не содержащие КВ, могут выполнять действия, на которые реагируют резидентные сторожа. Например, обычная команда LABEL изменяет данные в загрузочном секторе и вызывает срабатывание сторожа. Поэтому работа пользователя будет постоянно прерываться раздражающими сообщениями антивируса. Кроме того, пользователь должен будет каждый раз решать, вызвано ли это срабатывание компьютерным вирусом или нет. Как показывает практика, рано или поздно пользователь отключает резидентный сторож. И, наконец, еще один недостаток резидентных сторожей заключается в том, что они должны быть постоянно загружены в оперативную память и, следовательно, уменьшают объем памяти, доступной другим программам.

А.5 Основными недостатками метода вакцинирования являются возможность обхода такой защиты при использовании компьютерным вирусом так называемой «стелс-технологии», а также необходимость изменения кода программ, из-за чего некоторые программы начинают работать некорректно или могут перестать работать.

А.6 Аппаратно-программные методы представляют собой один из самых надежных способов защиты ПС от заражения КВ. Благодаря тому, что контроллер такой защиты подключен к системной шине компьютера, он получает полный контроль над всеми обращениями к дисковой подсистеме компьютера. Программное обеспечение аппаратной защиты позволяет указать области файловой системы, которые нельзя изменять. Пользователь может защитить главную загрузочную запись, загрузочные секторы, выполнимые файлы, файлы конфигурации и т.д. Если аппаратно-программный комплекс обнаружит, что какая-либо программа пытается нарушить установленную защиту, он может не только сообщить об этом пользователю, но и заблокировать дальнейшую работу компьютера.

Аппаратный уровень контроля за дисковой подсистемой компьютера не позволяет КВ замаскировать себя. Как только КВ проявит себя, он сразу будет обнаружен. При этом совершенно безразлично, как именно «работает» КВ и какие средства он использует для доступа к дискам и дискетам.

Аппаратно-программные средства защиты позволяют не только защитить компьютер от КВ, но также вовремя пресечь выполнение программ, нацеленных на разрушение файловой системы компьютера. Кроме того, аппаратно-программные средства позволяют защитить компьютер от неквалифицированного пользователя, не давая ему удалить важную информацию, переформатировать диск, изменить файлы конфигурации.

Недостатком аппаратно-программных методов является принципиальная возможность пропустить КВ, если они не пытаются изменять защищенные файлы и системные области.

УДК 681.3.06.001.4:006.354 ОКС 35.080 П85 ОКСТУ 4002

Ключевые слова: испытания программных средств, компьютерные вирусы, методы проведения испытаний программных средств, документация на испытания программных средств

Редактор *Л.В. Афанасенко*
Технический редактор *О.Н. Власова*
Корректор *В.И. Варенцова*
Компьютерная верстка *С.В. Рябовой*

Изд. лиц. № 021007 от 10.08.95. Сдано в набор 27.07.98. Подписано в печать 26.08.98. Усл.печ.л. 0,93. Уч.-изд.л. 0,76.
Тираж 420 экз. С 1037. Зак. 658.

ИПК Издательство стандартов, 107076, Москва, Колодезный пер., 14.
Набрано в Издательстве на ПЭВМ
Филиал ИПК Издательство стандартов — тип. "Московский печатник", Москва, Лялин пер., 6
Плр № 080102